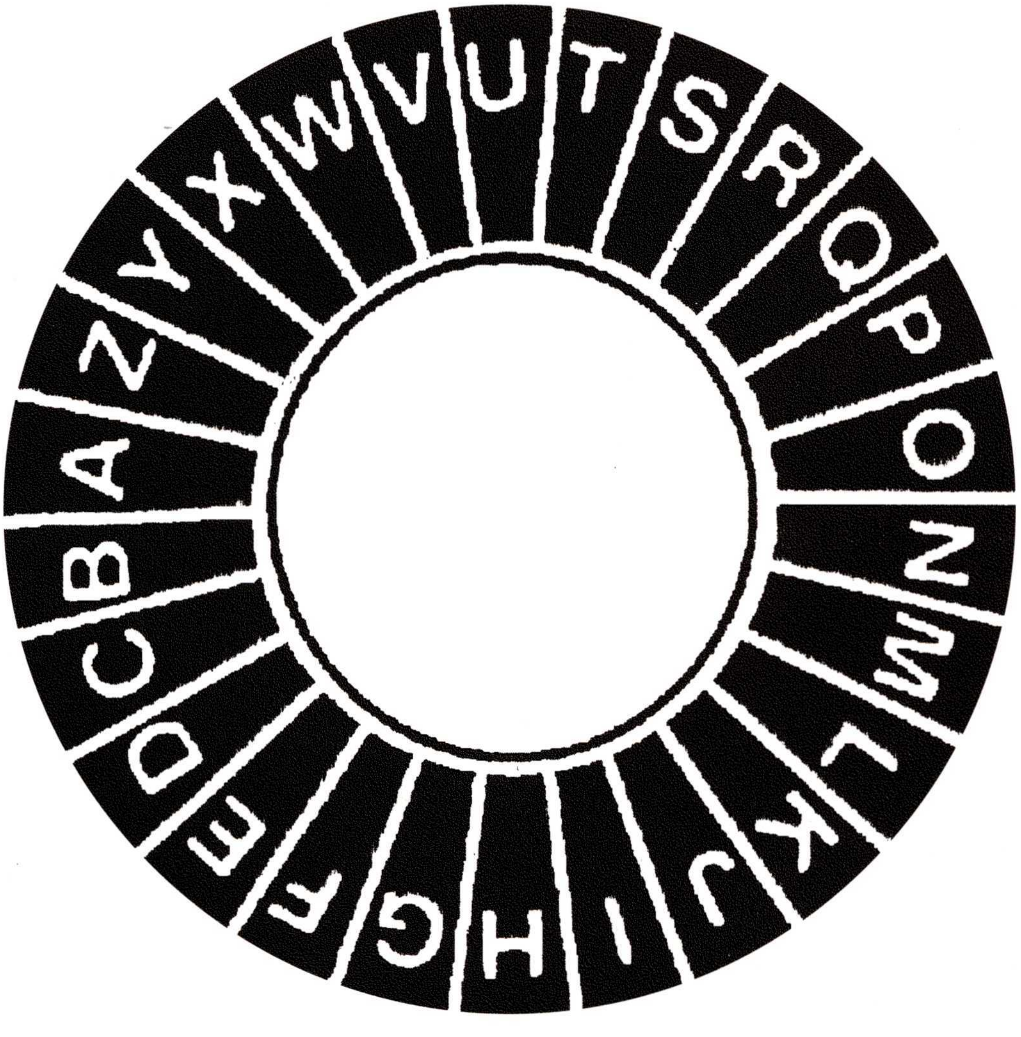
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Cryptologic
Excellence
— Yesterday, Today, and Tomorrow

CODES, CIPHERS, AND PUZZLES

ACTIVITY BOOK


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

THE CIPHER DISK
PRINTED ON THE INSIDE FRONT AND BACK COVERS

This simple device has a distinguished history. Ever since its first invention, it has been repeatedly reinvented in forms only slightly different from the original. Its story shows that man has sought to put the wheel to use in secret communications wherever possible, even as he also does in mechanics.

As invented in Italy sometime before 1470, it had similar concentric disks with the exception that one contained a "mixed" (scrambled) alphabet. Also in some of the earlier versions, one of two alphabets was composed of arbitrary symbols in lieu of conventional characters.

The appeal of the disk lay in the fact that with it, encipherment and decipherment could be performed without carrying bulky or compromising written materials.

The cipher disk came into large-scale use in the United States for the first time in the Civil War. The Federals' chief signal officer patented a version of it, very similar to the original Italian disk, for use in flag signaling. Since his flag stations were within the view of Confederate signalmen as often as not, he prescribed frequent changes of setting.

About a half-century later the U.S. Army adopted a simplified version, very similar to this device, in which one alphabet was "standard" and the other "reverse standard." Although technically this was a step backward, there were compensating advantages since the regularity of the alphabet tended to reduce error. During the period of the First World War and for several years afterward, the Army issued the disk in this form to units that needed a cipher which could be carried and used easily and which gave a few hours' protection to tactical messages.

In using this device, you could leave the two disks in the same setting for an entire message, thus producing the simplest possible cryptogram. Or their setting could be changed with every letter of the message and, if the patterns of the setting changes were complex enough, you would have an extremely secure cipher.

If you would like to make a cipher disk, and create secret communications, remove the front and back covers, cut out the two disks, and place the smaller disk on top of the larger one to create your message. You and a friend could secretly agree to a setting (place "C" on "f" for example) prior to exchanging messages. Remember you could agree to change the setting daily or weekly to make your messages more secure.

The Cipher Disk

Center for Cryptologic History

CAESAR CIPHER

Over two thousand years ago, Julius Caesar invented the simple cipher system that bears his name-Caesar-cipher. The Caesar cipher shifts the alphabet forward three places to create a new alphabet for sending secret messages.

Standard alphabet:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Caesar-shifted alphabet:

X Y Z A B C D E F G H I J K L M N O P Q R S T U V W

For example, if you wanted to write the message THE ENEMY IS NEAR in Caesar cipher, you would write QEB BKBJV FP KBXO. Try deciphering the following three messages using the Caesar cipher alphabet:

PMFBP PBKA PBZOBQ JBPPXDBP

QEB XOJV FP LK QEB JLSB

QELJXP GBCCBOPLK ABPFDKBA X PRYPQFQRQFLK ZFMEBO

ANSWERS: SEE BACK PAGE

LOGIC UNLOCKS PUZZLES

Often people who have a knack for solving cryptograms enjoy puzzles and logic problems as well. See how many of the following you can correctly answer. Solutions can be found on the back page.

When solving word puzzles, ask yourself the following questions:

1. What am I to find?
2. What facts do I have?
3. Are there special restrictions?
4. What relationships can I use?
5. Can I understand it better with a sketch or table or graph?
6. How shall I start?

Logic puzzle #1

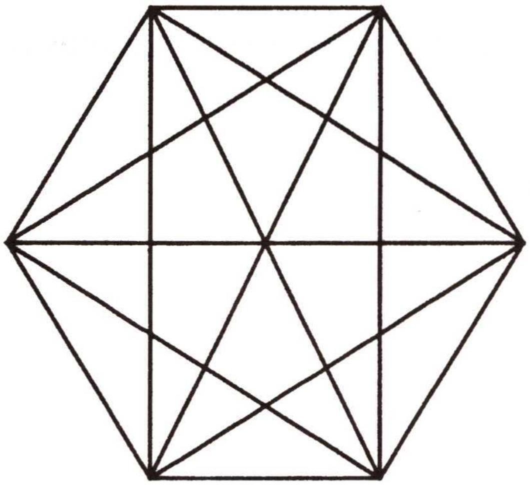
If a railroad train is moving northward, there is part of each car on that train that is moving southward at each instant, no matter how fast the train goes.

What is the contrary piece moving southward? Hint-sketch a train moving on a track and examine the parts you sketch.

Answer:

Logic puzzle #2

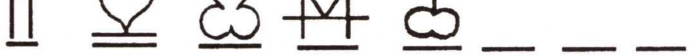
How many triangles can you find in this figure?



Answer:

Logic puzzle #3

What are the next three symbols in the series?



Logic puzzle #4

Can you make a walking man from 1 1 0 3 0 using only two straight lines?

Logic puzzle #5

"I have come to consult you," said the lawyer to the mathematician, "about Bill Brown's will. Bill Brown was fatally injured in a traffic accident while he was on his way to the hospital where his expectant wife was confined. He lived long enough to make a will, which provides that if his child is a boy the estate is to be divided in the proportion of two-thirds to the boy and one-third to the widow. But if the child is a girl, she is to receive only one-fourth and the widow receives the remaining three-quarters.

> "Now Mrs. Brown has given birth to twins, a boy and a girl. There is some question whether the will can be held to apply. What would be the correct division of the estate to carry out Brown's evident intentions?"

What was the mathematician's reply?

Answer:

Logic puzzle #6

Carol's ideal man is tall, dark and handsome. She dates Fred, George, Hank, and Joe: one of them is her ideal.

A. Each of the four has at least one desired trait.

B. Fred and George have the same complexion.

C. George and Hank are the same height.

D. Hank and Joe are not both tall

E. Only three of the men are tall, only two are dark, only one is handsome.

Who is Carol's ideal man?

Answer:

CRYPTO PUZZLE

This puzzle contains 35 words related to cryptology. You may know many of the words; you saw some of them in the museum, and several can be found in other activities in this booklet. The words read in any direction (including diagonal), and any letter may be used more than once. Six of the terms are compound words. Crypto puzzle answers can be found on the back page. Have fun!

```
Q W E R G U N I P A W C N D D J C V E I B A R K U F E L
C O D E S S Z A C Y G O L O T P Y R C E L M K E I J H S
S I E N J C C O M P R O M I S E D A S P L B Y Y I D E H
V E C I T P U R R G P P E I S H U L E E H W E T A W S E
N U I G S U K A A A G C R Y P T O G R A M A M A L T S E
G H P M X Z A S M M M R E L L E T Q U B U S B B T N W W
A R H A A Z B I Y B B L T P E C R E T N I P L L O E V I
S L E A A L P L D L C L Q U O P P V A T A E Y E B M Y T
F O R L L E A L P R O S E T T A S T O N E T R T U R N A
M E R M A S K E D C O M M U N I C A T I O N S N L E D E
C O D E B R E A K E R S D I G R A P H I C J X E J H I K
U T E C H N O L O G Y R E B M A H C K C A L B M P P A S
E T S E C R E T N G S H J O A W T S S T L L E R T I U A
L V E S O O P M M H T E B A H P L A O D O O C R E C A B
P A R R U E D P S S E U E W E E S O G G E T V H U N M P
R C W E R W I G W A G R A E L A N G I S A R H J M E P K
U N B T I R S Y J M A E S S T X A C C Y E B O M B E C A
P U T T E S P E T T A W C V E R A M R E R N T P O W E S
T C E H R I A K K E L L A S S R D H A Y B I E T S O B S
J A P C S E T C O D E T T A L K E R D S P C E E M A R T
A I X W F S C W A A C I O P E D I I I E T T A B A G I S
C L U S E H H E J J I R S C R Y P T O G R A P H Y S A M
```

FAMOUS PEOPLE IN CRYPTOLOGY
FROM THE MUSEUM'S EXHIBITS

______Albert J. Myer

______David Kahn

______Jean-Francois Champollion

______Abbot Johannes Trithemius

______Lawrence F. Safford

______Herbert O. Yardley

______Giovanni Battista Porta

______William F. Friedman

______Jacopo Silvestri

1. Called dean of American cryptology.
2. Author of first printed book on cryptology.
3. Author of second printed book on cryptology.
4. Called the father of modern cryptology.
5. Wrote *The Codebreakers.*
6. Used cryptanalytic techniques to unlock the key to the Rosetta Stone.
7. Called father of naval cryptology.
8. Army doctor who developed a visual line-of-sight flag system for battlefield telecommunications.
9. Directed MI-8, the first centralized cryptanalytic organization sponsored jointly by the Army and Department of State.

ANSWERS: SEE BACK PAGE

EXCERPTS FROM *YARDLEYGRAMS* BY HERBERT YARDLEY (1889–1958)

Herbert Yardley, as you may remember from the museum exhibit, was considered one of the most controversial figures in American cryptology. During his career, he served as a code clerk with the State Department, a military intelligence officer with the AEF, and as the initial chief of MI-8, the United States' first permanent centralized cryptanalytic organization. When MI-8 was closed down in 1929, due to budget cutbacks, Yardley published an unauthorized and revealing book (*The American Black Chamber*) about the activities of MI-8.

While this was Yardley's best known work, the following three stories, "The Mysterious Signals," "Self-Murder By Command," and "The Airplane Cipher," are taken from another Yardley book, *Yardleygrams*, published in 1932. The gist of the book was to teach the reader how to decipher cryptographic messages.

Yardley set the stage for his book by inventing the fictitious character Allan Crossle. His description of Crossle follows: "Allan Crossle, famous cipher expert and secret-ink chemist during the World War, and an ex-member of the now defunct American Black Chamber, has agreed to give his nephew, Charles Russell, an elementary course in cryptography. The course is to consist of a series of evening conferences at Crossle's home on Long Island. In order to stimulate his pupil's interest in the the subject, Crossle states each problem in the form of an unusual incident of espionage involving the solution of a cipher message. "

Perhaps you would like to try your hand at deciphering the messages. Keep in mind that the events in the stories took place during World War I (1914-1918), so some of the things described may be unfamiliar to you. If you enjoy solving the problems in these three stories, you might like to request a copy of Yardley's book from your local library. Good Luck in solving the cipher messages.

THE MYSTERIOUS SIGNALS

"During the close of the war," Crossle began at their initial meeting,"our secret wireless stations along the northern sector of the coast were interpreting a series of messages which, for a time, completely baffled every effort at decipherment. The signals always occurred at the same time-three o'clock in the morning, and were transmitted at such terrific speed that they came to us as an utterly unintelligible jargon. Direction finders indicated that they were coming from somewhere on the ocean, but the most vigilant patrolling of the Navy failed to disclose the presence of any suspicious vessel.

"Each night we recorded the signals on a phonograph record which was played over and over again in an effort to catch some inkling of the nature of the code. But we had absolutely no results. Then, one day the machine happened to run down and, to our astonishment, the jargon resolved itself into a perfectly intelligible sequence of letters. I am going to give you the very last message we received and let you try your skill," Crossle concluded. "Here it is."

snszk kxchr zakdc knmfh stcde nqsxk
zsht cdrdu dmsxs gqdd

Russell looked for several minutes at the array of five-letter groups. "How shall I go about it?" he asked, doubtfully. "There are two types of cipher," Crossle explained, "substitution and transposition. A transposition cipher is on in which the actual letters of the message have been transposed by a prearranged key. A substitution cipher is one in which the letters of the message have been changed to other letters or symbols. Later you will quickly discover the difference merely by inspection, but at first you should make a frequency table of each problem in order to determine whether you are dealing with a transposition or a substitution cipher. You make a frequency table by writing the alphabet A to Z and placing a mark after each letter in the alphabet for every occurrence of each letter in the message."

After a few minutes' work, Russell handed over the following frequency table of the cipher Crossle had given him: a-1, c-4, d-7, e-1, f-1, g-1, h-3, k-5, m-2, n-3, q-2, r-2, s-8, t-2, u-1, x-3, z-3.

"All right," Crossle said, "Note that k occurs five times, x and z each three times. From detailed analysis, we find that the letters jkqxz normally occur with the least frequency in any modern language-less than two percent of the total-while those of the group etaon occur most frequently. Therefore, the comparatively high frequency of k, x, and z in this message makes it certain we are dealing with a substitution cipher. To state it another way, these letters, since they occur so frequently, must represent other letters."

"That's clear enough," Russell admitted . "But now that I know it's a substitution cipher, what's the next step?"

"We always assume that any cipher is a simple one until proved otherwise. The simplest known cipher is the so-called Caesar alphabets, in which the letters of the message are represented by other letters, one, two, or three spaces forward or backward in the alphabet. That is, a may equal b, b equal c, and so on. To decipher such a message, one merely takes the first letter of the message, in this case, s, and continues the alphabet in vertical columns, s, t, u, v, etc. If you will follow this procedure with each letter, the message will be found in one of the horizontal lines."

SOLUTION

Russell returned to the desk and followed Crossle's instructions. Half an hour later he returned with a look of sheepishness.

"I don't seem to have any luck," he confessed, handing the worksheet over.

```
snszkkxchrzakdcknmfhstcdenqsxkzshstcdrdudmsxsgqdd
totallydisabledlongitudefortylatitudeseventythree
upubmmzejtbcmfempohjuvefgpsuzmbujuveftfwfouzuisff
vqvcnnafkucdngfnqpikvwfghqtvancvkvwfgugxgpvavjtgg
```

Crossle glanced at the sheet with a good-humored smile. "You'll be able to pick it out more readily when your eyes become accustomed to words jammed together. It reads: 'Totally disabled. Longitude forty, latitude seventy-three.'"

"What did you do about it?" Russell asked.

"A destroyer was immediately dispatched to the point designated and discovered that a German submarine had foundered in a depth of fifty fathoms. The messages, apparently, had been sent to another U-boat which was unable to render assistance in time. We sent a diver down who made an entrance by means of a dynamite charge and recovered many valuable German admiralty documents. Among those was a code book of the German Navy."

Frequency Table Worksheet

SELF-MURDER BY COMMAND

"It was the practice of the German Secret Service to keep its agents ignorant of one another's identities as far as possible," Crossle said. "In that way the capture of one did not lead to possible disclosures regarding any of the others. Occasionally, however, that had curious complications.

"I recall one bizarre case- a man named Sammis. We had strong suspicions that he was the spy referred to in several letters intercepted between other German agents as H-Seven. But despite all our vigilance we were unable to get anything on him. Then one afternoon he hurriedly left his office and went to his hotel room. One of our agents, stationed in an adjacent room, observed him through a peep-hole. Sammis paced about for a while, drew a letter from his pocket which he scrutinized in evident perturbation, then resumed pacing. Finally he got out a suitcase and began packing.

"Our agent started to open the connecting door, but the lock jammed and before he could enter Sammis escaped through the window. It was a sleety winter day and the fire-escape steps were encrusted with ice. Sammis slipped and fell, striking his head against the lower railing. He was taken to the hospital with a fractured skull and died a few hours later. He had previously torn the letter into bits which we pieced together. It was addressed to Sammis and contained routine instructions regarding a shipment of cotton-he was operating as a exporter to South America. But a cipher message inscribed in 'F' secret ink had been developed between the lines-apparently by Sammis himself that afternoon at his office. Here it is as your next problem."

The slip Crossle handed his pupil bore the letter groups:

nsrfq ctclm srnes gdvzx zsnmb d

"The first step of course," Crossle added, "is to make a frequency table to determine whether it's a substitution or a transposition cipher. If the former, then follow the same method of solution you used in the first problem."

SOLUTION

Russell spent the better part of an hour working over the message. Finally he said: " I find the words, 'Put H-Seven out,' on the third line but the rest of it's got me stumped."

Russell handed him the following:

nsrfqctclmsrnesgdvzxzsnmbd
otsgrdudmnts**ofthewayatonce**
puthsevenoutpguifxbzbupodf
qvuitfwfopvuqhvjgycacvqpeg

"If you will look in the second line," Crossle explained, "you will find the rest of the message. It reads, 'of the way at once.' In this type of cipher you may find the words in any one of the lines. For this reason it is well to complete the entire alphabet in the vertical columns."

"I'll remember that," Russell promised. "What's the meaning of the message?"

"It's an official order to do away with a spy whose continued existence was deemed dangerous to German espionage."

"Then Sammis really wasn't H-Seven?" Russell questioned.

"Unfortunately he was. And this message came as his own death warrant. Or more accurately, he was officially ordered to murder himself. What happened of course was that the sender of the order made a mistake-to him correspondents were merely so many code numbers-and he put the secret message on the letter to the victim instead of to his executioner." "But if Sammis had that message himself, wasn't he safe?" Russell objected.

"For the time being, yes. But the fact that he was a marked man naturally made him nervous. And so the poor devil assumed that our agent was his officially appointed assassin."

Frequency Table Worksheet

THE AIRPLANE CIPHER

"The most valuable information to the Germans was data regarding the movement of troops and ammunition from the United States to Europe," Crossle said at the next conference with Russell. "So naturally their spies used every conceivable device to that end, with an ingenuity that increased as our counterespionage grew more and more efficient. During the final period of the war, we were advised that an airplane had been making certain rather peculiar maneuvers off the south coast of Long Island. We sent one of our cryptographers over to make observations.

"It didn't take him long to discover what was going on. The pilot was, apparently, indulging in stunt flying . But by carefully following the trajectory of one tip of the wing, our observer was able to trace a series of letters such as the following:

rqvkm efaud xugrq ainag lipbc rokjj l

"This is a substitution cipher, as you can readily see," Crossle added. "It is made up with the Julius Caesar cipher, as were your first three ciphers. But I warn you that you will be unable to solve it unless you write down in vertical columns at least the first thirteen letters of the alphabet. Even then if you fail to search carefully, the message will escape you."

SOLUTION

After an hour's work Russell, crestfallen, admitted his failure. "It doesn't seem to make any sense," he said.

"You mustn't get discouraged so easily," Crossle said somewhat severely. "Many of the messages we had to deal with in the American Black Chamber took months of painstaking analysis. The chief asset of a successful cryptographer is a bulldog tenacity against seemingly insurmountable obstacles."

He took Russell's cross-section paper and underlined certain letters as follows:

```
rqvkmefaudxugrqainaglipbcrokjjl
srwlnfgbveyvhsrbjobhmjqcdsplkkm
tsxmoghcwfzwitsckpcinkrdstqmlln
utynphidxgaxjutdlqdjolsefurnmmo
vuzoqijeyhbykvuemrekpmtfgvsonnp
wvaprjkfziczlwvfnsflqnughwtpooq
xwbqsklgajdamxwgotgmrovhi uqppr
yxcrtlmhbkebny hpuhnspwij   qqs
zydsumniclfco  iqviotqxjk      t
      ojdmgdp       urykl     u
         nheq        szlm
          ifr        tamn
           gs        ubno
            t
```

" '*S.S. York*-midnight-ten thousand troops,' " Russell read slowly. "That's rather a tough one."

"You'll learn to spot the message readily with practice," Crossle reassured him. "The message was received by a U-boat off the Long Island coast, probably through a telescope."

"Who was the airplane pilot?" Russell asked.

"An army instructor at Roosevelt Field-a chap with an excellent record in every respect. Which goes to prove that when it comes to espionage no one is above suspicion."

Frequency Table Workshop

✖ = A
✔ = B
✣ = C
➤ = D
➔ = E
✜ = F
✧ = G
★ = H
☆ = I
↔ = J
✉ = K
● = L
○ = M
■ = N
✼ = O
✚ = P
✱ = Q
❒ = R
▲ = S
✳ = T
◆ = U
↕ = V
◗ = W
✪ = X
❖ = Y
✝ = Z

EASY

Write the correct letters in the blanks

___ ___ ___   ___ ___ ___
✣ ✖ ■   ❖ ✼ ◆

___ ___ ___ ___   ___ ___ ___ ___
❒ ➔ ✖ ➤   ✳ ★ ☆ ▲

___ ___ ___ ___ ___ ___
▲ ➔ ✣ ❒ ➔ ✳

___ ___ ___ ___ ___ ___ ___ ?
○ ➔ ▲ ▲ ✖ ✧ ➔

Now write a secret message
of your own!

INTERMEDIATE

A cryptogram is a puzzle in which each letter in a sentence is replaced by a different letter of the alphabet. The three sentences below are cryptograms. See if you can solve them. Think of what the sentences might be saying and look for letter patterns that match the words that you think might be there. Write the letters that you think belong in the sentence in the spaces over each cryptogram. Watch out, though! We used a different way of replacing letters in each sentence (which means that if you guess the "U" in the first cryptogram is really the letter "R", then the "U" in the second and third cryptogram will NOT be an "R"; it will be a different letter).

If you need some hints to get started, look at the bottom of the page.

1. UJTUQJ FQQ FWTZSI YMJ BTWQI QNPJ YT XTQAJ UZEEQJX.

2. MIGY JOTTFYM WUH VY BULX NI MIFPY, VON MIGY ULY YUMS.

3. QVQ LBH GUVAX GUNG GUVF CHMMYR JNF UNEQ BE RNFL GB QB?

The letters in the cryptogram are called "cipher" letters, and the letters that you wrote down are called "plain" letters. Fill in as much of the chart below as you can, writing the cipher letters under the correct plain letter. Do you see any patterns?

Plain: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher 1: --

Cipher 2: --

Cipher 3: --

Hints:

1. *Look for a pattern that would fit the word "PEOPLE."*
2. *The word "SOME" appears twice in this sentence.*
3. *Three words in a row begin with "TH."*

ADVANCED

Each of the following cryptograms was produced by first creating a keyword-mixed alphabet. In a keyword-mixed alphabet, a word is selected ("FOOTBALL," for example), any repeated letters are dropped (the second "O" and the second "L'"to make "FOTBAL"), and the word is followed by the rest of the unused letters in the alphabet (to make the final sequence "FOTBALCDEGHIJKMNPQRSUVWXYZ"). This sequence is then slid to the left or right some number of positions (allowing the sequence to "wrap around'"to the other end where necessary) to create a substitution 'code'. Each cryptogram uses a different slide, which is determined by the letters in a "setting" word, which is written vertically beneath the first letter of the keyword-mixed alphabet. For example, given the keyword FOOTBALL and the setting word PUNT, the substitution set-up would be:

Plain: F O T B A L C D E G H I J K M N P Q R S U V W X Y Z
Cipher 1: P Q R S U V W X Y Z F O T B A L C D E G H I J K M N
Cipher 1: U V W X Y Z F O T B A L C D E G H I J K M N P Q R S
Cipher 3: N P Q R S U V W X Y Z F O T B A L C D E G H I J K M
Cipher 4: T B A L C D E G H I J K M N P Q R S U V W X Y Z F O

If we were to use a different slide for each sentence, we could encipher 4 sentences with this set-up.

Below are 5 cryptograms for you to solve. They were created using the process described above, but with a different keyword and setting word. (HMMMMM....there are 5 cryptograms. How long would the setting word have to be?)

1. LHKUFXKUL, J LXYIRU ETMMRU KJD NU KJQU TE HV LUOUBJR EJBFL.
2. KEON MEGS FCHS IK HBWRKJ QX BGJKG SB OBFK SB E OBFMWKSK HBWCSQBX.
3. VGT OANRV UZNV WO VGAR UFKKBT AR RWBHADX VGT LNQUVWXNZCR VGTCRTBHTR.
4. IMQC XRK TKOC AMCMWTDIM CBM FMXNRWA KOMA CR TDQ CBM PHZBPGMC.
5. TNUJTH, HKA QAUJ ZRLAFX KAJ JCX SKFW AUXW ZKF JCX UXJJROL.

Answers to Easy, Intermediate, and Advanced puzzles can be found on the back page.

ANSWERS TO THE CAESAR CIPHER

SPIES SEND SECRET MESSAGES

THE ARMY IS ON THE MOVE

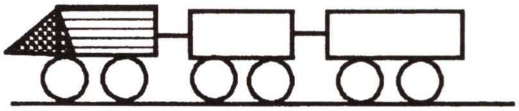
THOMAS JEFFERSON DESIGNED A SUBSTITUTION CIPHER

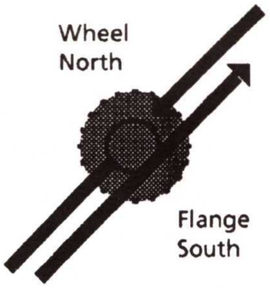
ANSWERS TO LOGIC UNLOCKS PUZZLES

Logic puzzle #1

The contrary piece on each car is the flange of the wheel. The flange lies below the rail and moves south as the wheel turns.

Sketch of train:



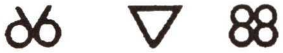


Logic puzzle #2

We found 110 triangles; can you find any we missed?

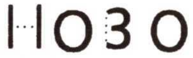
Logic puzzle #3

The symbols are mirror images of the numbers 1 2 3 4 5; therefore, the next three symbols would be mirror images of 6 7 8.



Logic puzzle #4

HOBO



Logic puzzle # 5

Bill's intention was to give his wife half as much as his son. He wanted to give his wife three times as much as his daughter.

Wife's share: **W = 1/2S**

Estate = Wife's + Son's + Daughter's

3D + 6D + D

10D

Daughter's share = 1/10 of estate

Wife's share = 3/10 of estate

Son's share = 6/10 of estate

Logic puzzle #6

If George and Hank are the same height, they must be tall. Then Joe is short and the third tall man is Fred. Joe must be dark or handsome or both. Suppose that Joe were handsome, he would be the only handsome man. Joe can't be the ideal man because he is short, so someone else is handsome. Joe is dark, and one other man is dark. Then Fred and George have the same complexion (fair). So only Hank is dark and tall. Hank must be handsome and be the ideal man.

ANSWERS TO CRYPTO PUZZLE

WORDS ACROSS BACKWARD AND FORWARD

CODE

CRYPTOLOGY

COMPROMISED

WHEEL

CRYPTOGRAM

INTERCEPT

ROSETTA STONE

MASK

COMMUNICATIONS

CODE BREAKERS

DIGRAPHIC

TECHNOLOGY

BLACK CHAMBER

SECRET

WIG WAG

SIGNAL

BOMBE

CODE TALKER

CRYPTOGRAPHY

SIGABA

ALPHABET

(21)

DIAGONAL WORDS

LOGIC

ENCRYPT

SCRAMBLE

CIPHER

(4)

WORDS STRAIGHT UP AND DOWN

ENCIPHERMENT

KEY TABLE

DISPATCH

COURIER

PURPLE

RADIO

PUZZLE

ENIGMA

DECIPHER

JADE

(10)

ANSWERS TO FAMOUS PEOPLE IN CRYPTOLOGY

____8__Albert J. Myer

____5__David Kahn

____6__Jean-Francois Champollion
____2__Abbot Johannes Trithemius
____7__Lawrence F. Safford
____9__Herbert O. Yardley
____4__Giovanni Battista Porta
____1__William F. Friedman
____3__Jacopo Silvestri

ANSWER TO EASY PUZZLE: CAN YOU READ THIS ANSWER?

ANSWERS TO INTERMEDIATE PUZZLE:
1. PEOPLE ALL AROUND THE WORLD LIKE TO SOLVE PUZZLES

2. SOME PUZZLES CAN BE HARD TO SOLVE, BUT SOME ARE EASY.

3. DID YOU THINK THIS PUZZLE WAS HARD OR EASY TO DO?

ANSWERS TO ADVANCED PUZZLES:
1. SOMETIMES, A SINGLE PUZZLE MAY BE MADE UP OF SEVERAL PARTS.
LHKUFXKUL, J LXYIRU ETMMRU KJD NU KJQU TE HV LUOUBJR EJBFL.

2. EACH PART MUST BE SOLVED IN ORDER TO COME TO A COMPLETE SOLUTION.
KEON MEGS FCHS IK HBWRKJ QX BGJKG SB OBFK SB E OBFMWKSK HBWCSQBX.

3. THE FIRST PART OF THIS PUZZLE IS SOLVING THE CRYPTOGRAMS THEMSELVES.
VGT OANRV UZNV WO VGAR UFKKBT AR RWBHADX VGT LNQUVWXNZCR VGTCRTBHTR.

4. NEXT YOU MUST DETERMINE THE KEYWORD USED TO MIX THE ALPHABET.
IMQC XRK TKOC AMCMWTDIM CBM FMXNRWA KOMA CR TDQ CBM PHZBPGMC.

5. LASTLY, YOU MUST FIGURE OUT THE WORD USED FOR THE SETTING.
TNUJTH, HKA QAUJ ZRLAFX KAJ JCX SKFW AUXW ZKF JCX UXJJROL.

PA: CRYPTOGAMS BDEFHIJKLNQUVWXZ

C1: SBDEFHIJKLNQUVWXZCRYPTOGAM
C2: OGAMSBDEFHIJKLNQUVWXZCRYPT
C3: LNQUVWXZCRYPTOGAMSBDEFHIJK
C4: VWXZCRYPTOGAMSBDEFHIJKLNQU
C5: EFHIJKLNQUVWXZCRYPTOGAMSBD

KEY WORD: CRYPTOGRAMS
SETTING WORD: SOLVE

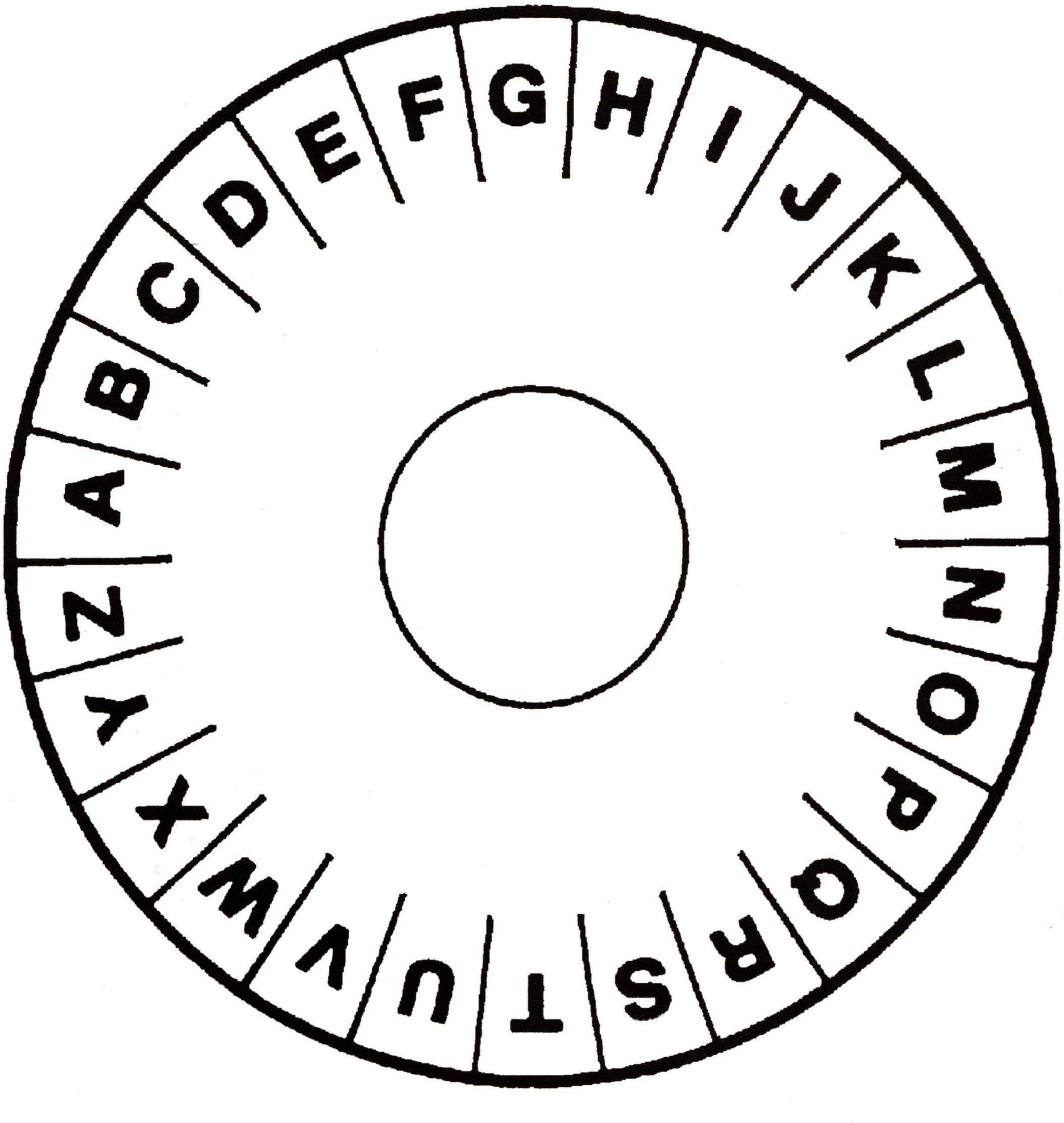
ATTRIBUTION:

Yardleygrams, Herbert O. Yardley, The Bobbs-Merrill Company, Copyright, 1932. Copyright expired.

Logic Unlocks Puzzles copyright 1979 by the University of Oklahoma. Copied here with permission from the University of Oklahoma: "This material was prepared with the partial financial support of the National Science Foundation under Grant Number ED75-02213, and of the University of Oklahoma. However, opinions, findings, conclusions, and recommendations expressed herein are those of the authors, and do not necessarily reflect the views of the National Foundation or the University of Oklahoma."

Easy, Intermediate, and Advanced Puzzles prepared by Larry Gray.

All other materials compiled by the staff of the Center for Cryptologic History.


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z

i27889